REMARKS

The above-identified application is United States application serial number 10/749,200 filed on December 31, 2003. Claims 1-31 are pending in the application. Claims 1-31 are rejected.

Rejection of Claims under 35 U.S.C. §103

Claims 1-3, 7-10, 11-13, 16-21, and 24-31 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas in view of Coppersmith. Applicants have amended the claims. The amended claims distinguish over Matyas in view of Coppersmith at least because the references do not disclose input text blocks including a first input text block that receives a first plaintext block derived from a secret PIN and a second input text block that receives a second plaintext block derived from a non-secret entity-identifier that is independent of the PIN. **FIGUREs 1A** and **1B** and associated paragraphs [0017]-[0031] the entity-identifier's characteristic independence from the PIN, the characteristic which is further stressed, for example, in paragraph [0049] where the institution that enrolls the customer account (the entity-identifier) does not possess the PIN. Matyas describes a system and technique (see column 22, lines 50-54) wherein a first input to the cryptographic algorithm is the PIN (in common with applicants' claimed system) but a second input is an IBM 3624-formatted PIN that is derived from validation data and a PIN validation key (which is derived from the PIN – specifically contrary to applicants' claims). The technique disclosed by Matyas thus results in the difficulties raised by the applicants in paragraph [0007] wherein:

> "If a PIN is compromised, then an adversary can use the PIN offset to compute a new PIN chosen by the customer. Accordingly, selection of the new PIN does not attain security once a PIN is compromised. The only way to recover security is for the bank or other issuing entity to change either the customer account number or the bank's PIN verification key. Changing the customer account number is difficult for the bank, and changing the PIN verification key is even more difficult. Accordingly, an easy attack against that PIN is available."

Coppersmith is also silent with regard to one of the cryptographic algorithm's inputs being an identity-identifier which is independent of the PIN.

Claims 4-5 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas in view of Coppersmith and Vernam (1310719). The amended claims distinguish over Matyas in view of Coppersmith and Vernam which fail to disclose inputs to a cryptographic algorithm including a first plaintext block derived from a secret PIN and a second plaintext block derived from a non-secret entity-identifier that is independent of the PIN. The Examiner admits that Matyas and Coppersmith do not teach a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block, but states that Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext. Applicants believe Vernam does not teach first and second ciphertexts that are formed and combined to produce a ciphertext, but rather merely discloses combination of a plaintext block with a ciphertext block. Accordingly, the combination of Matyas, Coppersmith and Vernam, does not combine signals and thus does not operate as claimed by the applicants. Regarding Claim 5, the combination of Matyas, Coppersmith, and Vernam neither describes nor hints of recovery of the secret PIN from the second ciphertext block as claimed or operation in the irreversible mode as claimed.

Claims 6, 15, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas in view of Coppersmith and Vernam, and further in view of Briachtl. The amended claims distinguish over Matyas in view of Coppersmith, Vernam, and Briachtl which fail to disclose inputs to a cryptographic algorithm including a first plaintext block derived from a secret PIN and a second plaintext block derived from a non-secret entity-identifier that is independent of the PIN. The claims further distinguish over the references because, while Briachtl discloses the general concept of escrow storage, the combined references do not teach storing a ciphertext block in the escrow storage to facilitate recovery of the secret PIN.

Claims 14 and 22 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas in view of Coppersmith and Vernam (1310719). The amended claims distinguish over Matyas in view of Coppersmith and Vernam which fail to disclose

inputs to a cryptographic algorithm including a first plaintext block derived from a secret PIN and a second plaintext block derived from a non-secret entity-identifier that is independent of the PIN.

CONCLUSION

The application, including all remaining Claims 1-31, is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at (949) 251-0250.

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, Central Number at (571) 273-8300 on the date shown below:

/Joy C. Ngo
(Signature)

Joy C. Ngo
(Printed Name of Person Signing Certificate)

September 9, 2009
(Date)

Respectfully submitted,

/Ken J. Koestner/

Ken J. Koestner
Attorney for Applicant(s)
Reg. No. 33,004